인터넷 패킷 보호 보증 플랫폼에서의 보안성 평가 시스템 설계

(Design of the Security Evaluation System for Internet Secure Connectivity Assurance Platform)

김 상 춘 † 한 근 희 ††
(Sang Choon Kim) (Keun Hee Han)

요 약 IPsec은 네트워크 계층에서 정보보호 서비스를 제공하기 위한 프로토콜이다. 현재 IPsec을 기반으로 하는 인터넷 패킷 보호 보증 플랫폼들이 다양한 환경에서 구현되고 있다. 그러나 현재까지 IPsec을 기반으로 하는 시스템에 대한 보안성을 평가하는 기술이나 연구는 미약한 실정이다. 따라서 본 논문에서는 IPsec을 기반으로 하는 인터넷 패킷 보호 보증 플랫폼(ISCAP: Internet Secure Connectivity Assurance Platform)의 보안성을 평가하기 위한 보안성 평가 시스템을 설계 및 구현하였다. 본 평가 시스템은 ISCAP의 보안성을 평가하여 보안 취약점을 도출하는 것에 더하여, IPsec을 기반으로 하는 시스템 개발 시 디버깅 도구로도 활용될 수 있을 것이다.

키워드 : 보안성 평가 시스템, IPsec 프로토콜, 보안 취약성

Abstract IPsec protocol has been developed to provide security services to Internet. Recently IPsec is implemented on the various operating systems. Hence, it is very important to evaluate the stability of the IPsec protocol as well as other protocols that provide security services. However, there has been little effort to develop the tools that require to evaluate the stability of IPsec protocols. Therefore, in this paper, we develope the security requirements and suggest a security evaluation system for the Internet packet protection protocols that provide security services at the IP level that can be used to check if the security protocols provide the claimed services correctly. This system can be used as debugging tool fordeveloping IPsec based security system.

Key words : security evaluation system, IPsec protocol, Security Vulnerability

1. 서 론

1.1 개요

인터넷과 WWW의 이용이 폭발적으로 증가하면서 인터넷 정보보호 프로토콜에 대한 많은 연구가 진행되어 왔다. 지금까지 인터넷 응용분야에 대표적인 정보보호 메커니즘으로는 전자우편 부문에 PGP, PEM, S-MIME, 네트워크 관리 부문에 SNMP 보안, 웹 부문에 S-HTTP, SSL/TLS와 SOCKS 등을 들 수 있다. IETF에서는 TCP/IP 네트워크를 대상으로 전송 계층과 네트워크 계층에 표준 정보보호 메커니즘을 제공하고자 노력을 계속하고 있다. IPsec 프로토콜은 이러한 노력의 일환으로 1994년 7월에 IETF의 IPsec Working Group에서 RFC로 제안한 표준이다. 현재 IPsec 프로토콜은 17개의 RFC와 28개의 Internet-draft 문서로 제안되어 있다. 이러한 IPsec 프로토콜은 현재 여러 운영체제에서 시험 중에 있고 IKE를 포함한 완벽한 구현은 아니지만, VPN 서비스를 위한 제품으로 상용화되고 있다. IPsec이 인터넷 정보보호 서비스에서 차지하는 역할은 IPsec과 가장 유사한 서비스 기능을 가지고 있고 또한 현재 널리 사용되고 있는 SSL과의 비교를 통해서 알 수 있다.

SSL은 전송 계층에 적용되어 서버와 클라이언트 통신에 암호화 서비스를 제공한다. 그러나 SSL은 TCP에 적용되기 때문에 UDP를 사용하는 응용프로그램들에게는 아무런 정보보호 서비스를 제공할 수가 없으며 이는 차세대 인터넷에서 중요성이 부각되고 있는 멀티캐스팅을 이용한 응용프로그램들에게는 커다란 단점이 될 수 있다. 멀티캐스팅은 Ack Explosion 등과 같은 문제점

† 종신회원 : 삼척대학교 정보통신공학과 교수
kimsc@samcheok.ac.kr
†† 종신회원 : 공주대학교 응용수학과 교수
kehan@kongju.ac.kr
논문접수 : 2003년 5월 15일
심사완료 : 2003년 12월 20일

때문에 TCP가 아닌 UDP를 사용하고 있다.

IPsec은 IP 계층에서 정보보호 서비스를 제공한다. TCP/IP를 이용하는 모든 통신은 반드시 IP 계층을 거쳐가야 하기 때문에 IPsec은 응용프로그램이 TCP나 UDP 중 어느 프로토콜을 사용하는 지와 무관하게 정보보호 서비스를 제공한다. 즉 IPsec의 정보보호 서비스를 사용하기 위하여 응용프로그램들을 변경할 사항이 전혀 없다는 것이다.

이러한 IP레벨의 정보보호 서비스를 제공하기 위하여 개발되는 시스템은 일반적인 시스템보다 보안성 유지가 매우 중요하기 때문에 이를 위해서는 시스템에 대한 보안성 평가가 필요하다. 보안성 평가를 위해서는 많은 종류의 보안성 시험과 분석이 요구된다. 보안성 평가 시스템은 보안성 시험을 통해 보안상의 문제점을 찾아내고, 이를 바탕으로 보안 상태를 향상시킬 수 있도록 보안상 문제점을 해결할 수 있는 방법을 제시해 주는 시스템이다. 또한 침입탐지 시스템처럼 공격자의 침입이 일어난 시점에서 사건을 분석하여 이를 방어하기 보다는 시스템의 상태를 분석하여 시스템 전체의 보안 상태를 평가하고 이에 대한 해결책을 제시함으로써 불법적인 행동이 발생하기 전에 시스템의 보안 수준을 높여줄 수 있는 시스템이다[1,2].

1.2 보안성 평가 시스템 연구의 필요성

현재까지 IPsec 엔진에 대한 보안성을 평가하기 위한 자동화된 도구는 나와있지 않다. 보안 호스트에 대한 보안 취약성 분석 툴로 AXENT의 NetRecon[3], Cisco의 Cisco Scanner[4] 그리고 LANguard network&port scanner[5] 등이 있으나, 이러한 툴들은 단지 호스트나 네트워크에 대한 스캐닝 기능만을 제공하며 실제 IPsec 보안 서비스를 제공하는 특정 호스트에 대한 보안성을 평가하는 기능은 제공해 주지 못한다.

또한 sscan, SATAN, SAINT, ISS 등의 해킹 툴을 사용하여 시스템 및 네트워크의 취약점을 분석하는 방법도 널리 사용되고 있으나 각각의 툴을 하나로 통합하여 사용하기가 불편하고 각각의 보안상 취약점을 통합 분석한 종합적인 분석 결과를 얻어내기 힘들며 새로운 취약점이 알려질 때마다 각각의 툴들을 따로 업데이트 해야 하는 단점이 있다. 이러한 툴들 역시 IP 계층의 보안 서비스에 대한 평가는 수행하지 못한다[6].

이처럼 현재 IP 계층의 보안서비스에 대한 보안성 평가를 위한 정형화되고 표준화된 기술은 아직 없는 실정이다.

따라서 IPsec의 보안성 분석을 위한 보안성 평가 시스템에 대한 보다 심화된 연구와 개발이 필요하다.

본 논문에서는 이러한 연구의 일환으로 IPsec을 기반으로 하는 ISCAP의 보안성을 평가하기 위한 보안성 평가 시스템을 설계 및 구현하였다. 본 평가 시스템은 ISCAP의 보안성을 평가하여 보안 취약점을 도출하는 것에 더하여, IPsec을 기반으로 하는 시스템 개발 시 디버깅 도구로도 활용될 수 있을 것이다.

2. 관련연구

2.1 인터넷 패킷 보호 보증 플랫폼의 보안 요구사항

ISCAP에서는 IP 계층에서 정보보호 서비스를 제공한다. 따라서 상위 계층의 프로토콜은 수정할 필요가 없다.

IP레벨에서 IPv4/IPv6를 지원하는 IPsec Engine은 다음과 같은 정보보호 서비스를 제공할 것이 요구된다[6-8].

가. 기밀성(confidentiality)

메시지를 암호화하여 키를 가진 합법적인 사람을 제외하고는 중간에 불법적인 도청자가 메시지의 내용을 알아볼 수 없도록 하는 서비스이다.

나. 무결성(integrity)

메시지 변조를 할 수 없도록 하는 것으로 송신자가 메시지를 특정 수신자에게 전송할 경우 제3자가 불법적인 도청을 통해 전송한 메시지를 중간에서 가로챈 후 메시지를 변조하여 수신자에게 전송할 수 없도록 하는 서비스이다.

다. 데이타인증(data authentication)

서로를 직접 확인할 수 없는 인터넷상에서 상대에 대한 신뢰를 확보하기 위해 제공되는 서비스이다.

라. 접근 제어(access control)

불법적인 제3자의 접근을 완전히 차단하거나, 서로 다른 중요도를 가지는 정보 및 시스템에 대해서 접근 권한을 달리 부여하여 정보를 보호하는 서비스이다.

마. 재현공격방지(Anti-replay)

한 번 사용된 메시지를 다시 사용할 수 없도록 하는 서비스로써, 송신자가 수신자에게 보낸 메시지를 중간에서 제3자가 가로채고 있다가 메시지 수신이 일단 완료된 후에 가로챈 메시지를 다시 보내 공격하는 것을 막는 서비스이다.

2.2 인터넷 패킷 보호 보증 플랫폼

인터넷 패킷 보호 보증 플랫폼(ISCAP : Internet Secure Connectivity Assurance Platform)은 IP레벨 보안 서비스를 제공하는 시스템으로 IPsec을 기반으로 하는 시스템이다. IPv4/IPv6를 지원하는 IPsec Engine은 IP레벨에서 기밀성(confidentiality), 무결성(integrity), 데이타 인증(data authentication), 접근 제어(access control), Anti-replay서비스 등을 응용레벨 인터넷 서비스에 제공한다. 이는 IP계층에서 정보보호 서비스를 제공하므로 상위 레벨 프로토콜 및 프로그램을

수정할 필요가 없다.

ISCAP의 각 서브시스템은 공개키 기반 시스템(PKI: Public Key Infrastructure)에서 제공하는 CA(Certification Authority)와 연동을 통하여 공개 키 인증에 관한 정보를 교환하며, IPsec을 지원하는 VPN 서버, 라우터, 방화벽 시스템과의 연동을 통하여 정보보호 서비스를 제공한다.

ISCAP 시스템은 IPsec 프로토콜에 대한 IETF의 표준 문서를 기초로 개발되고 있으며, 본 논문에서는 이러한 표준 문서에서 정의된 사항을 토대로 하여 ISCAP의 구조를 분석하였다. 또한 구조 분석을 위해 ETRI에서 개발한 IPsec 기반의 통합 정보보호 시스템 C-ISCAP(Controlled Internet Secure Connectivity Assurance Platform)의 구조를 참조 하였다[13].

2.2.1 시스템 형상

ISCAP 시스템에서 제공할 기능들을 그룹화하면 그림 1과 같이 IP 보안 연결 호스트 시스템(ISHS : IP Secure connectivity Host System), IP 보안 연결 게이트웨이 시스템(ISGS : IP Secure connectivity Gateway System), IP 보안 연결 콘트롤 시스템(ISCS : IP Security Control System) 등 3개의 서브시스템으로 구성되며, 각 서브시스템은 인터넷에 접속되어 인터넷을 통해 IP 패킷 형태로 상호간의 정보를 교환한다. 이러한 형상 구성도는 그림 1과 같다.

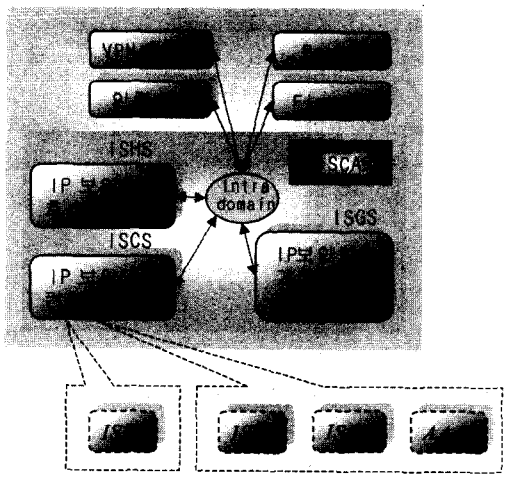


그림 1 인터넷 패킷 보호 보증 플랫폼(ISCAP) 형상 구성도

2.2.2 서브시스템과 블록 연관도

ISCAP 시스템은 3개의 서브시스템과 여러 블록으로 구성되며 서브시스템과 블록의 연관도는 그림 2와 같다.

2.2.3 서브 시스템의 기능

그림 2의 ISCAP를 구성하는 각 서브시스템의 기능은 다음과 같다.

가. IP 보안 연결 호스트 서브시스템

(ISHS: IP Secure connectivity Host System)

ISHS는 IP 보안호스트 기능, 통합 키 관리 기능, 자동 키 교환 기능, 보안기반 규칙 제어 클라이언트 기능, 보안관리 클라이언트 기능과 보안연계성 데이타베이스(SAD: Security Association Database), 보안기반 규칙 데이타베이스(SPD: Security Policy Database)로 구성된다. 이러한 기능을 통하여 호스트에서 송/수신되는 데이타의 기밀성, 무결성, 접근 제어, IP 데이타그램에 대한 발신지 인증, 선택적인 Anti-Replay 서비스 등의 정보보호 서비스를 제공한다.

나. IP 보안 연결 게이트웨이 서브시스템

(ISGS:IP Secure connectivity Gateway System)

ISGS는 IP 보안게이트웨이 기능, 통합 키 관리 기능, 자동 키 교환 기능, 보안기반 규칙 제어 클라이언트 기능, 보안관리 클라이언트 기능과 SAD, SPD로 구성된다. 이러한 기능을 통하여 게이트웨이에서 송/수신되는 데이타의 기밀성, 무결성, 접근제어, IP 데이타그램에 대한 발신지 인증, 선택적인 Anti-Replay 서비스 등의 정보보호 서비스를 제공한다.

다. 보안기반 규칙 제어 서브시스템

(ISCS: IP Security Control System)

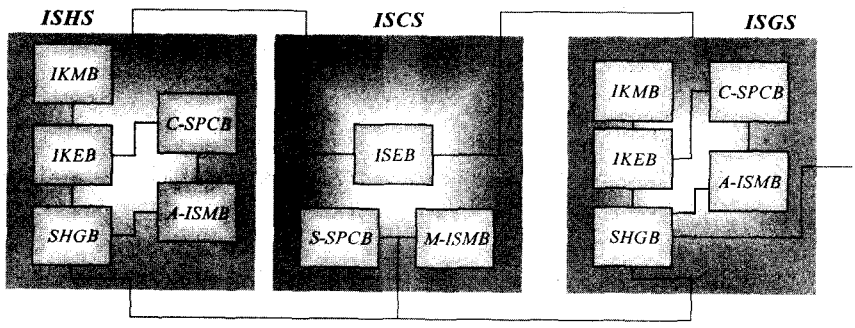


그림 2 ISCAP 각 서브 시스템과 블록의 연관도

ISCS는 보안기반 규칙 설정 기능, 보안취약성 분석 기능, 통합관리 모니터링 기능으로 구성된다. 각 기능들은 ISCAP의 구성 요소들을 통합적으로 제어하는 역할을 하며 호스트와 호스트, 호스트와 게이트웨이, 게이트웨이와 게이트웨이간의 비밀 통신을 연결하기 위하여 종단간의 비밀통신 기반 규칙 설정 및 정보 교환을 수행한다. 또한 ISCAP 내의 보안상 취약점 분석과 감사 이벤트 처리, 시스템 및 IP 데이타의 모니터링을 통하여 보안상 문제점을 찾아내고 이를 운용자에게 보고함으로써 보안 관리자가 문제점을 해결할 수 있도록 서비스를 제공한다.

2.2.4 블록의 기능

ISCAP를 구성하는 각 서브시스템내의 블록의 기능은 다음과 같다.

가. 보안호스트/게이트웨이 블록

(SHGB : Secure Host/Gateway Block)

SHGB는 SPD의 기반 규칙을 준수하여 송신 호스트와 수신 호스트, 송신 호스트와 게이트웨이, 게이트웨이와 수신 호스트, 게이트웨이와 게이트웨이간의 보안 연결을 수행한다. 본 블록에서는 임의의 시스템(호스트 또는 게이트웨이)간의 보안 연결을 설정한 후 데이타를 교환하기 위하여 보안기반 규칙 설정 기능을 통해 보안기반 규칙을 수립한 후 자동 키 협상 기능을 이용하여 두 시스템 사이의 SA(Security Association)를 설정한다.

나. 인터넷 키 교환 블록

(IKEB : Internet Key Exchange Block)

IKEB는 안전한 방법으로 SA와 인증된 키 재료의 협상 및 키 제공을 수행하는 기능으로 원격지에 있는 사용자가 보안성을 갖춘 호스트나 게이트웨이를 통하여 네트워크에 접근할 수 있도록 한다.

다. 인터넷 키 관리 블록

(IKMB : Internet Key Management Block)

IKMB는 자동 키 협상 기능에 의해 생성된 키를 등록, 갱신, 저장, 삭제 및 키 데이타베이스 관리, 멀티캐스팅 키 관리, 키 위탁 및 복구, 자동 키 협상 기능에 의해 설정된 SA의 저장 및 관리를 수행한다.

라. 보안기반 규칙 제어 블록

(SPCB : Security Policy Control Block)

SPCB는 보안 호스트와 보안 게이트웨이에게 다중 게이트웨이를 통한 안전한 통신 채널을 설정하기 위해서 필요한 기반 규칙 정보를 생성, 제공한다. 보안기반 규칙 설정 기능을 통해서 각 보안 호스트는 보안 게이트웨이를 식별하고, 이들 게이트웨이들이 시작 호스트 또는 목적 호스트에 대한 권한 여부를 검증한다.

마. 인터넷 보안 관리 블록

(ISMB:Internet Security Management Block)

ISMB는 패스워드, 접속 조절 명단, 보안 로그, 암호화 장치 등에 관련된 정보를 모니터링하고 통제한다. 본 블록에서는 감사 이벤트 처리, 형상 관리, IP 모니터링, SA 모니터링, 통계처리, Recovery, 운용자와의 인터페이스 기능을 제공한다.

3. 보안성 평가 시스템 설계

이 절에서는 관련 연구에서 분석한 인터넷 패킷 보호 보증 플랫폼에서의 보안성을 평가하여 보안상의 위협을 도출하고, 이를 관리자에게 알려줄 수 있고, 확장성을 갖는 보안성 평가 시스템을 설계하기 위한 기능 요구사항들을 도출하고 이를 충족시키기 위한 보안성 평가 시스템을 설계한다.

3.1 보안성 평가 시스템에 대한 기능 요구사항

이 논문에서 설계하는 인터넷 패킷 보호 보증 플랫폼에서의 보안성 평가 시스템에 대한 기능요구사항은 다음과 같다.

- ISCAP의 안전성 분석이 가능해야 한다.
- 다양한 운영체제에서 보안성 평가 기능을 수행할 수 있어야 한다.
- 평가 룰 데이타베이스의 보안성 평가 룰을 사용한 룰 기반의 보안성 평가가 가능해야 한다.
- 보안성 평가 룰 관리 기능, 즉 룰의 추가, 삭제, 변경 등이 가능해야 한다.
- 관리자 툴을 사용한 중앙 집중식 관리를 제공해야 한다.
- GUI를 이용한 ISCAP의 취약점 상황 디스플레이가 가능해야 한다.
- Security Hole 발견 시 찾은 과정을 리포트하는 기능을 수행할 수 있어야 한다.
- 보안성 평가 후 시스템 설정 수정 권유를 할 수 있어야 한다.
- 에이전트를 이용한 특정 호스트의 low level 수준에서의 보안성 분석을 할 수 있어야 한다.
- 특정 서브넷의 보안성 평가를 할 수 있어야 한다.
- 각 서브넷의 모든 평가 정보를 수집해 전체 도메인의 보안성을 평가할 수 있어야 한다.
- 평가 기능을 모듈화하여 손쉽게 업그레이드할 수 있도록 하여야 한다.
- 지정시간에 자동으로 수행이 가능해야 한다.

3.2 보안성 평가 시스템의 구조 및 기능 흐름도

위의 기능 요구사항을 만족시키기 위하여 이 논문에서 제안하는 보안성 평가 시스템의 구조 및 기능 흐름도는 그림 3과 같다.

이러한 보안성 평가 시스템을 구성하는 블록의 내부 구조 및 흐름도는 그림 4와 같다.

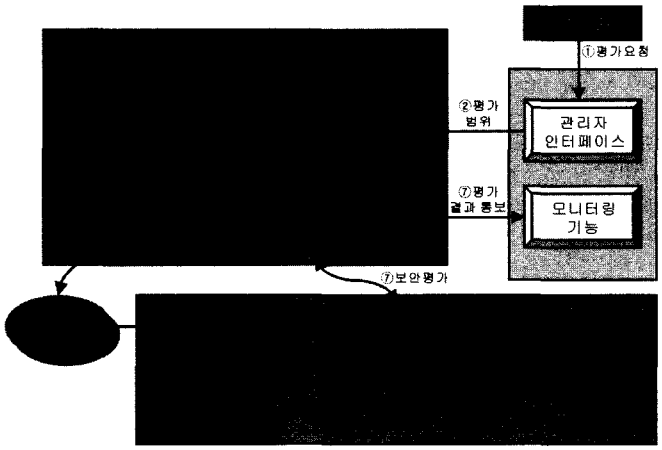


그림 3 보안성 평가 시스템의 구조 및 기능 흐름도

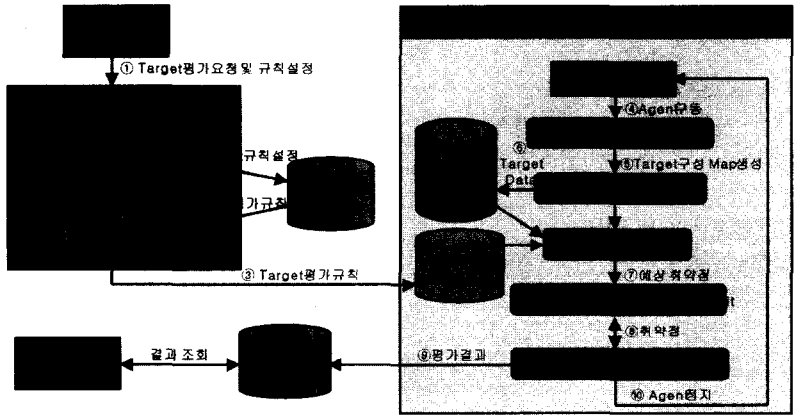


그림 4 보안성 평가 시스템의 블록 내부 구조 및 흐름도

블록을 구성하는 각 요소들에 대한 세부 기능에 대한 정의는 다음과 같다.

가. 규칙제어 모듈

(Rule Control Module ; RCM)

관리자가 GUI를 통해 보안성 평가 환경을 설정하거나, 보안규칙 DB의 보안성 평가 규칙을 관리하거나, 관리자가 설정한 보안성 평가 범위 및 대상에 해당하는 보안성 평가 규칙을 설정하여 주는 기능을 하는 모듈로서, GUI와 보안성 평가 규칙 DB, 규칙 평가 모듈과 연동한다.

- 규칙설정 유니트(Rule Setting Unit ; RSU)
  - GUI를 이용하여 보안성 평가에 관한 규칙들을 추가 및 변경, 삭제 기능
- 평가대상 설정 유니트
  (Target Selecting Unit ; TSU)
  - GUI를 이용하여 평가 대상 및 평가 범위를 설정하는 기능
  - 설정된 평가 대상과 범위에 관련된 규칙을 보안성 평가 규칙 DB에서 선정하여 평가규칙 Store에 저장하는 기능

나. 규칙 평가 모듈

(Rule Evaluation Module ; REM)

평가대상군의 네트워크 연결 현황을 파악하고, 평가대상군으로부터 평가에 필요한 데이타를 수집하여, 분석한 후 예상취약점을 도출하는 기능과 도출된 예상 취약점을 평가하여 취약점을 확인하는 기능을 하는 모듈로서, 평가 결과를 평가 결과 DB에 저장하고 GUI를 통해 관리자에게 알려주는 기능을 포함한다. 또한 규칙제어 모듈, 평가 결과 DB 및 GUI와 연동한다.

- 네트워크 현황 유니트

(Network Mapping Unit ; NMU)

- 모든 포트와 IP주소를 검색하여 현재의 네트워크 연결 상태를 정의하는 기능

- 데이타 수집 유니트
  (Data Collection Unit ; DCU)
  - 현재의 네트워크 연결 상태를 참조하여 모든 호스트와 네트워크 디바이스로부터 평가 대상 자료를 가져와 Target Data Store에 저장하는 기능
- 데이타 분석 유니트
  (Data Analysis Unit; DAU)
  - 평가 규칙 Store에 저장된 평가규칙을 Target Data Store에 저장된 자료에 적용하여 취약점을 분석한 후 예상되는 취약점을 알아내는 기능
- 취약점 확인 유니트
  (Vulnerability Confirmation Unit ; VCU)
  - 예상취약점에 대해 실제취약점이 존재하는지를 네트워크에 직접 침입하여 조사하는 기능
- 취약점 결과보고 유니트
  (Vulnerability Reporting Unit VRU)
  - 평가 결과에 대한 사항을 항목별로 정리하여 평가 결과 DB에 저장하고, GUI 통하여 결과를 출력하는 기능

3.3 보안성 평가 시스템의 수행 절차

보안성 평가 시스템의 처리절차는 다음과 같다.

<평가요청 수행 절차>

[관리자 -> GUI] 관리자가 GUI를 통해 평가 대상 및 규칙을 설정한다.

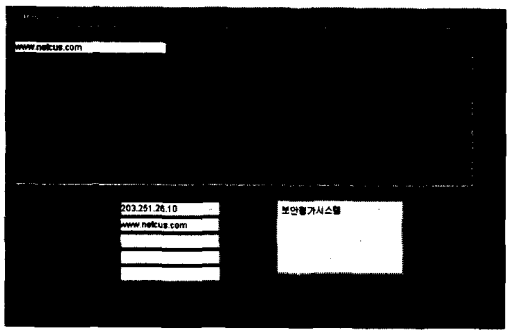


그림 5 평가 대상 설정

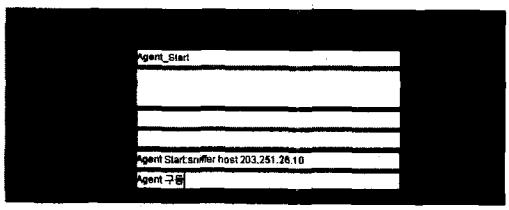


그림 6 평가 규칙 설정

<RCM 수행 절차>

[단계 1] GUI를 통해 관리자가 설정한 평가 대상 및 규칙을 보안성 평가규칙 DB에 저장한다.

[단계 2] 보안성 평가규칙 DB로부터 관리자가 요청한 평가 대상에 대한 규칙을 수집하여 평가 규칙 Data Store에 저장한다.

그림 7 평가 대상 선택

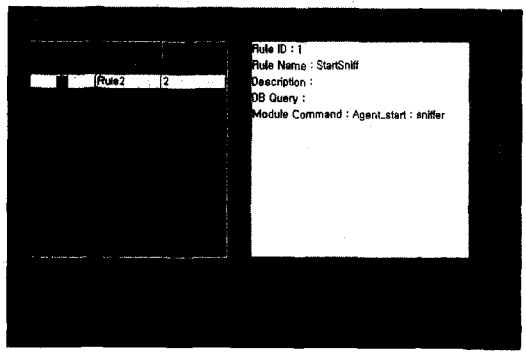


그림 8 평가 규칙 선택

<REM 수행절차>

[단계 1] 보안성 평가 Agent을 구동한다.

[단계 2] 평가대상 네트워크 구성도를 생성한다.

[단계 3] [단계 2]에서 생성된 평가 대상에 관련된 Data를 수집하여 평가 대상 Data Store에 저장한다.

[단계 4] 평가규칙 데이타 Store에 저장된 규칙을 평가 대상 Data Store에 저장된 데이타에 적용하여 평가한다.

[단계 5] 평가한 결과를 통해 예상 취약점을 도출한다.

[단계 6] 발견된 취약점의 평가 결과를 평가결과 DB에 저장하고 결과를 출력한다.

[단계 7] 보안성 평가 Agent을 정지한다.

<기타 수행절차>

[단계] 관리자는 필요할 때 언제든지 GUI를 통해 평가 결과 DB를 검색한다.

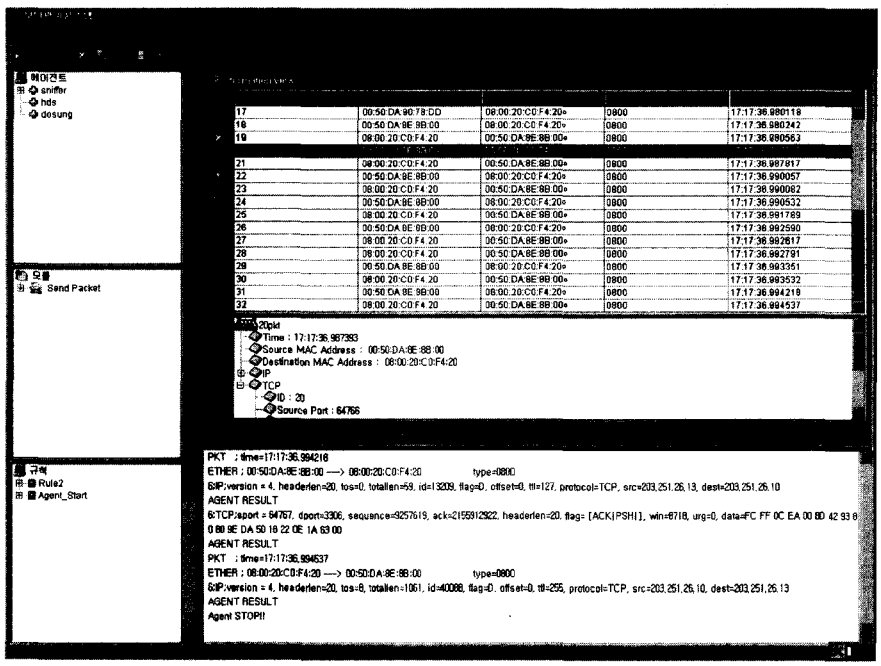


그림 9 평가 대상으로부터 수집된 패킷 데이타

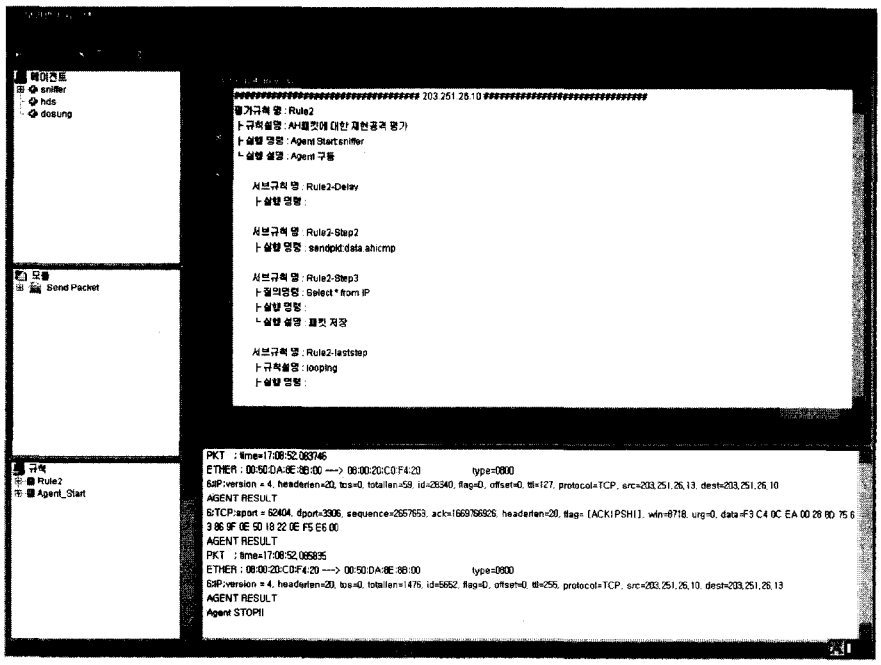


그림 10 평가규칙 실행

4. 보안성 평가

본 논문에서 제안한 보안성 평가 시스템과 에이전트에 탑재된 패킷 스니핑 모듈은 JAVA와 C를 통해 구현하였다. 데이타베이스는 my-sql로 구현하였다.

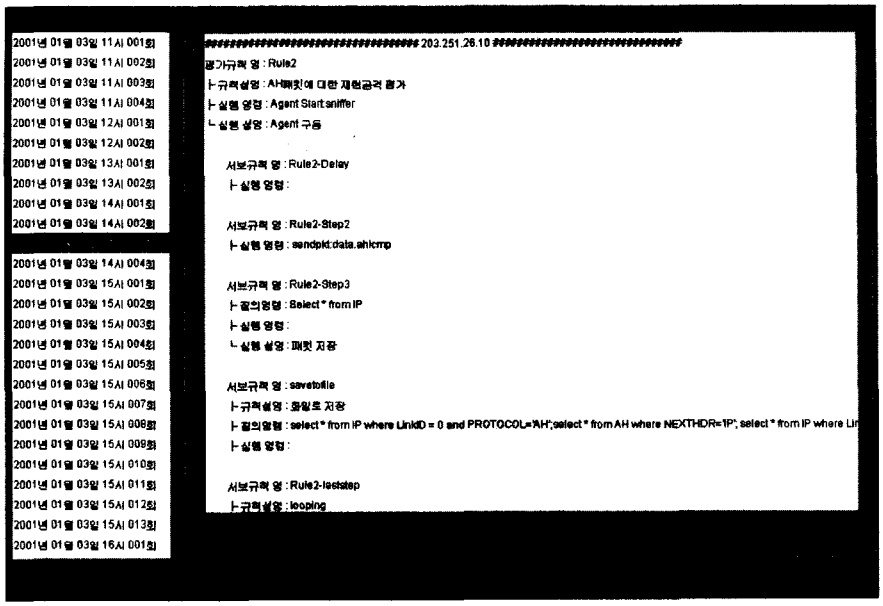


그림 11 평가 결과 검색 보기

IPsec에서 제공하는 5가지 보안성을 인터넷 패킷 보호 보증 플랫폼이 적절히 제공하는지를 평가 시스템을 통하여 평가하기 위한 방법을 요약하면 다음과 같다.

• 기밀성(confidentiality)

전송중인 암호화된 ESP 패킷을 수집하여 메시지의 내용을 알아 볼 수 있는지 확인하고 임의의 키를 생성하여 복호화 해본다.

• 원적지 인증(Data Origin Authentication)

전송중인 AH 혹은 ESP 패킷을 실시간으로 수집한 후 수집한 패킷 헤더 내의 전송자의 IP 주소를 공격자의 주소로 변경하여 목적지로 전송하고, 이 패킷을 받은 노드가 이에 대한 응답을 하는지 확인한다.

• 접근 제어(Access Control)

임의의 키(key)를 이용하여 AH 혹은 ESP 패킷을 구성하여 목적지로 패킷들을 전송하여 접근 권한을 얻을 수 있는지 시도한다.

• 비연결형 무결성(Connnectionless Integrity)

네트워크 상에서 실시간으로 수집한 패킷의 특정 필드를 임의로 변경한 후 ICV값을 재계산하여 변조하여 전송하고, 이에 대한 대상 노드의 응답이 있는지 확인한다.

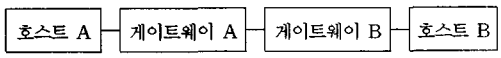
• 재현공격 방어(Anti-replay)

네트워크 상에서 실시간으로 수집한 패킷을 다시 동일한 목적지로 전송하여 본다. 또는 수집된 패킷의 IPsec AH/ESP 헤더내의 SN(Sequence Number)값을 감시하여, 새로운 SN을 생성하거나 수집한 SN을 변경하여 재전송하고, 이에 대해 대상 노드의 응답이 있는지 확인한다.

본 논문에서는 이상의 5가지 기본적인 보안 서비스의 제공 및 IPsec의 정상동작을 테스트하기 위해 50가지의 항목으로 구성된 테스트 suite을 정의하여 ISCAP을 평가하여 보았다.

50가지의 평가 항목 중 두 가지 항목만 간단히 소개하면 다음과 같다.

시스템 구성 :



[항목 1] Tunnel AH의 원적지 인증 테스트

방법 :

<절차 1> 호스트 A에서 Tunnel AH가 적용된 ICMP 패킷을 생성하여 호스트 B로 전송한다.

<절차 2> 보안성 평가시스템은 이 패킷을 실시간으로 sniffing하여 원적지 주소를 변경한 후 호스트 B로 전송한다.

<절차 3> 보안성 평가시스템은 sniffing 모듈을 통해 호스트 B가 이 패킷에 대한 응답 패킷을 호스트 A로 보내는지를 확인한다.

<절차 4> 만약 호스트 B가 응답패킷을 보냈다면, Tunnel AH의 원적지 인증서비스에 대한 보안 취약성이 있으므로, 이를 보안 관리자에게 통보하여 준다.

[항목 2] SA bundle 동작 테스트

방법 :

<절차 1> 호스트 A와 호스트 B 사이는 Transport AH, 게이트웨이 A와 게이트웨이 B 사이는 Tunnel ESP가 적용되도록 정책을 설정한다.

<절차 2> 호스트 A에서 호스트 B로 ICMP 패킷을 생성하여 전송한다.

<절차 3> 보안성 평가시스템은 sniffing 모듈을 통해 패킷들을 캡쳐하여 다음을 확인한다.

- 호스트 A와 게이트웨이 A 사이의 패킷이 Transport AH가 적용된 패킷인지
- 게이트웨이 A와 게이트웨이 B 사이의 패킷이 Tunnel ESP가 적용된 패킷인지
- 호스트 B와 게이트웨이 B 사이의 패킷이 Transport AH가 적용된 패킷인지

<절차 4> ICMP 패킷을 받은 호스트가 이에 대한 응답 패킷을 보냈고, 이 패킷이 호스트 A에 전달되었는지를 스니핑된 패킷을 통해 확인한다.

<절차 5> 만약 <절차 3> 및 <절차 4>의 패킷이 모두 확인되었다면 SA bundle이 정상 동작함이 확인된 것이다.

위에서 [항목 2]의 경우는 SA bundle의 동작을 테스트 한 것이며 SA 번들에 대한 보안성 테스트 항목도 따로 존재한다.

실제로 ETRI 에서 개발한 C-ISCAP을 평가대상으로 하여 보안성 평가를 수행하여 보았다. 테스트 결과 C-ISCAP는 50개의 아이템 중 46개의 아이템을 통과하였다. 통과하지 못한 4개의 아이템은 C-ISACP에서 구현을 마치지 못한 SA bundle에 대한 것이었다.

5. 결 론

본 논문에서는 IP 레벨에서의 정보보호 서비스를 제공하기 위한 인터넷 패킷 보호 보증 플랫폼에 대한 시스템 형상 및 각 구성 요소들의 기능과 각 프로토콜이 제공하는 정보보호 서비스에 대하여 분석하고, ISCAP이 제공하는 정보보호 서비스에 대한 보안성을 평가하기 위한 시스템 요구사항을 도출하고, 이를 충족하는 보안성 평가 시스템을 설계 및 구현하였다.

제안한 보안성 평가 시스템은 인터넷 패킷 보호 보증 플랫폼에서 요구되는 정보보호 서비스에 대한 보안성을 평가하기 위한 기술들을 정의하고, 정의한 기술들을 이용하여 ISCAP의 보안성을 평가하여 그 결과를 저장하고, 관리자가 필요시 그 결과를 참조할 수 있는 기능을 갖는다.

본 평가 시스템은 JAVA, C, my-sql을 통해 구현되었으며 실제 50개의 테스트 아이템을 만들어 ETRI에서 개발한 C-ISCAP에 대해 보안성 평가를 수행하여 보았다.

본 평가 시스템은 ISCAP의 보안성을 평가하여 보안 취약점을 도출하는 것에 더하여, IPsec을 기반으로 하는 시스템 개발 시 디버깅 도구로도 활용될 수 있을 것이다.

본 평가 시스템은 3.1절의 기능 요구사항을 만족하도록 설계 및 구현하였으나, 일부 요구사항에 대하여는 충족되지 못한 부분이 있다. 이 부분에 대해서는 향후 보완해 나갈 예정이다. 이와 관련하여 보완할 내용은 평가 시스템이 좀 더 다양한 운영체제에서 동작하도록 하는 것 - 현재는 Linux와 Solaris에서만 동작 - 그리고 보안성 평가 후 시스템 설정을 수정할 것을 권유하는 기능 추가에 대한 것이다.

이에 더하여 향후 과제로서 좀 더 다양한 ISCAP에 대한 보안성 평가를 시도하여 본 평가시스템의 기능을 보완하는 작업이 필요하며, 취약성 데이타 베이스와의 연동을 통해 좀 더 확장성 있는 평가 시스템이 될 수 있는 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] 이재승, 김상춘, 이종태, 김경범, 손승원, "대규모 네트워크 환경하에서의 침해사고 예방을 위한 보안성 평가 시스템 설계", 제12회 정보 보호와 암호에 관한 학술대회(WISC 2000), pp. 160~176, 2000.

[2] FreeS/WAN, http://www.ipv6.iabg.de/

[3] ISS, Network and Host-based Vulnerability Assesment, AXENT, http://www.axcent.com

[4] Cisco Scanner, http://www.cisco.com/univercd/cc/td/doc/pcat/nssq.htm

[5] LANguard Network&Port scanner, http://www.gfi.com/languard/lanscan.htm

[6] Larry J. Hughes, Jr., Actually Useful Internet Security Techniques, New Riders Publishing, 1995.

[7] IETF RFC2401, "Security Architecture for the Internet Protocol".

[8] IETF RFC2402, "IP Authentication Header(AH)".

[9] IETF RFC2406, "IP Encapsulating Security Payload(ESP)".

[10] IETF RFC2407, "The Internet IP Security Domain of Interpretation for ISAKMP".

[11] IETF RFC2408, "ISAKMP"

[12] IETF RFC2409, "The Internet Key Exchange(IKE)".

[13] J.H.Jeong, J.H.Nah, S.W.Sohn and J.T.Lee, "C-ISCAP: Controlled-Internet Secure Connectivity Assurance Platform," Proc. of the IEEE International Conference on Enterprise Information Systems(ICEIS2001), Vol. 2, pp. 920-925, Setubal, Protugal.

[14] Kane Security Analyst Product Home Page, http://www.mantech.co.kr/ksa.html

[15] Inzen Home Page, http://www.inzen.com
[16] 이재승, 김상춘, 김경범, 손승원, "대규모 네트워크 보안성 분석 자동화를 위한 보안성 평가 시스템의 설계", 제5회 통신소프트웨어 학술대회 COMSW2000 (The 5thConference on communication Software), pp. 172~176.
[17] Vulnerability Testing, http://esperosun.chungnam.ac.kr/~jmkim/firewall/vulnerability/vul00.html
[18] 한국전산원, "정보시스템 보안을 위한 위험 분석 소프트웨어 개발 보고서", 1997.

김 상 춘

1986년 한밭대학교 전자계산학과(공학사) 1989년 청주대학교 전자계산학과(공학석사). 1999년 충북대학교 전자계산학과(이학박사). 1983년~2001년 한국전자통신연구원 정보보호 연구본부(선임기술원). 2001년 7월~현재 전자통신연구원 정보보호 연구본부 초빙연구원. 2001년 4월~현재 삼척대학교 정보통신공학과 조교수

한 근 희

1986년 건국대학교 물리학과(학사). 1991년 University of Central Oklahoma 응용수학과(석사). 1996년 University of Oklahoma 컴퓨터과학과(박사). 1996년~2000년 한국전자통신연구원 정보보호 연구본부(선임연구원). 1999년~2000년 National Institute of Science and Technology(NIST) (객원연구원). 2000년~현재 공주대학교 응용수학과 조교수